

# Information Services Risk Assessment at UMBC: A Case Study

Robin Anderson

[robin@umbc.edu](mailto:robin@umbc.edu)



# A Little About Me...

- ◆ Data Communications / Security Specialist with the Office of Information Technology at UMBC
- ◆ Instructor in Secure UNIX System Administration and SANS Level One Security courses at UMBC





# Goals

- ◆ Outline core Information Services Risk Assessment (ISRA) requirements & processes
- ◆ Fit ISRAs into the context of the larger organization
- ◆ Scale ISRAs to meet time & personnel constraints, security requirements, and organizational standards



# Topics

- ◆ Theory
  - Definitions
  - Basic ISRA Processes
- ◆ Developing Our Process: OIT's Odyssey
  - Scaling the Endeavor
- ◆ Case Study: Assessing UMBC's Financial Aid Department
- ◆ Online Resources





# Theory



# Guidelines for Definitions

- ◆ Crucial to be *clear* and *precise* when defining terms
  - Importance of internal consistency
  - Local jargon phrases may have wholly different meanings elsewhere
- ◆ Misunderstandings can cost hours of time and incalculable goodwill





# Risk Management vs. Risk Assessment

## ◆ Risk Management:

- Overarching discipline, includes RA
- Whole service department dedicated to RM

## ◆ Risk Assessment:

- Much more proscribed endeavor
- Deals with specific departments
- Deals with specific risks



# What is Risk?

*Threats* that are *likely* to:

- manifest
- allow access to a *vulnerable asset*
- cause damage

and sometimes:

- have *mitigating* safeguards





# What is Risk? (2)

## ◆ Iteration 1:

- $\text{Threat}_1 = \text{Likelihood} \times \text{Vulnerability}$
- $\text{Risk}_1 = \text{Threat}_1 \times \text{Impact}$

## ◆ Iteration 2:

- $\text{Threat}_2 = (\text{Likelihood} \times \text{Vulnerability}) - \text{Mitigations}$
- $\text{Risk}_2 = \text{Threat}_2 \times \text{Impact}$



# Components of Risk

## ◆ Threat

- Events that have the potential to compromise information assets, composed of *Likelihood*, *Vulnerability*, and *Mitigations*

## ◆ Impact

- Severity of consequences in the event of *asset* compromise





# Components of Threat

- ◆ Likelihood
  - Probability of event occurring
- ◆ Vulnerability
  - Capability (possibly *mitigated*) of threatening vector to access protected *asset*
- ◆ Mitigations
  - Factors which reduce *threat* to protected *asset* (usually partially rather than totally)



# More Definitions

## ◆ Asset

- Potentially *vulnerable* information which must be protected from *threats*

## ◆ Acceptance of Risk

- Decision that further *mitigations* are not justified by predicted *impact*





# Sources of Risk

- ◆ Physical: Environmental conditions
- ◆ Network: Traffic flow impediments, network application abuse
- ◆ System: Physical storage components of information flow
- ◆ People: Users, administrators, intruders



# From Theory to Fact-Finding

- ◆ Going from general theory of risk to finding concrete ways of isolating, evaluating, and addressing risk locally
- ◆ Many different choices
  - Qualitative vs. quantitative
  - One-time vs. short-term progressive vs. longitudinal





# Basic ISRA Processes

- ◆ Focusing scope
- ◆ Gathering information
- ◆ Determining *Critical Assets*
- ◆ Assessing *Threats*
- ◆ Proposing *Mitigations*
- ◆ Communicating results



# Developing Our Process:

## OIT's Odyssey





# Federal Regulations

- ◆ Legislatively-mandated deadlines for regulatory compliance
  - Gramm-Leach Bliley Act (GLBA)
    - Covers financial institution customer information
    - Compliance by May 23, 2003
  - Health Insurance Portability & Accountability Act (HIPAA)
    - Covers health care provider customer information
    - Compliance by April 21, 2005



# Deadlines, Deadlines

We were considering formal risk assessments for the first time in early 2003...

... and it turned out we had an implementation deadline of May 23<sup>rd</sup>, 2003!





# Constraints & Challenges

- ◆ Short time to delivery
- ◆ Small number of staff (1) working on project
- ◆ Highly ambiguous requirements
  - No guidelines or checklists in regulations
  - Greater overhead associated with developing assessment system
- ◆ Need for standardization
  - ISRAs had to have same format & consistent approach across areas assessed



# Trade-Offs

- ◆ Development Time  $\Leftrightarrow$  Execution Time
  - More Development Time  $\Rightarrow$  More Standardization
  - More Standardization  $\Rightarrow$  More Consistent Results
- ◆ Overall Time  $\Leftrightarrow$  Assessment Depth
  - More Depth  $\Rightarrow$  More Accuracy *(hopefully)*





# An Iterative Approach

1. Define specific end goals & conditions
  - Format of final process
  - Time to complete one-time assessment
  - Acceptable levels of complexity
2. Research
  - Similar organizations' processes
  - Security and auditing group recommendations
3. Create broad preliminary composite
  - Highlight possible directions for management



# An Iterative Approach (2)

4. Management and developers form consensus on direction & what can be removed
5. Cut out all excess material discovered in Step #4 and simplify
6. Refine existing material and develop new material as necessary
7. Repeat from Step #4 until end conditions from Step #1 are met





# OIT's Current Process:

The Condensed Five-Phase  
Quantified ISRA Methodology



# The Five Phases

1. Define critical asset at risk / to be protected
2. Develop local information flow model
  - A. Identify data storage points
  - B. Identify data transmissions
  - C. Identify discrete steps in flow





# The Five Phases (2)

3. Identify & evaluate risks associated with local information flows
  - A. Identify risk(s) associated with each step of the flow model from Step 2
  - B. Evaluate identified risk(s): Simplified Risk Quantification Methodology (SRQM) Iteration 1
  - C. Generate a risk-levels matrix
  - D. Determine acceptable risk-levels



# The Five Phases (3)

4. Develop mitigation strategy to address non-zero risk matrix elements
5. Generate Final Risk Levels Matrix and Mitigations & Findings Reports
  - A. Re-evaluate remaining risk(s): SRQM Iteration 2
  - B. Generate final risk-levels matrix
  - C. Generate mitigations & formal findings report



# Case Study:

## Assessing UMBC's Financial Aid Department



# Implementation

- ◆ Outlined scope of project
- ◆ Met with Financial Aid to acquire background information to facilitate following the Five Phases
- ◆ Moved on to Five Phases





# Implementation: Phase 1

## 1. Define critical asset(s)

- Derived from GLBA requirements
- Met with Financial Aid
  - Assessed outstanding information
  - Identified instances of GLBA-defined assets
    - Included students' identifying information, financial records, etc.
- ✓ List of assets defined



# Implementation: Phase 2

## 2. Develop local information flow model

### A. Identify data storage points

- In FA: mainframes, servers, desktops
- At UMBC: campus servers & systems
- Off-campus: Gov't servers, home computers

### B. Identify data transmissions

### C. Identify discrete steps in flow

- ✓ Local information flow model developed  
(see next slide)





# FA Entity Communication Matrix

Entity Communication Matrix

OIT / Financial Aid IT Risk Assessment

Destination

Source

		Mainframe			Central Server		FA Desktops		Other UMBC			Off-Campus		
		SIS	SAFERS	SAR	EDEExpress	SAFERS	Standard	Privileged	Campus MX Servers	Campus Interactive Login Servers	Other Campus Servers and Systems	US D of Ed/SAFERS	FA Users' Home Systems	External Systems & Servers
Mainframe	SIS		X											
	SAFERS			X										
	SAR		[X]											
Central Server	EDEExpress											X		
	SAFERS		X											
FA Desktops	Standard	?	?	?					X	X		?		X
	Privileged	X	X	X	X	X			X	X		X		X
Other UMBC	Campus MX Servers								X	[X]	[X]		[X]	[X]
	Campus Home Dir Servers	?	?	?					X	X	[X]	?	[X]	
	Other Campus Servers and Systems	?	?	?	?	?			X	X	[X]	?	[X]	
Off-Campus	US D of Ed/SAFERS				X									
	FA Users' Home Systems	?	?	?			?	?	X	X	[X]	?	[X]	X
	External Systems & Servers	?	?	?			?	?	X	X	[X]	?	[X]	X

Note: Based on 'new' network organization scheme

Key	?	Outstanding question(s)
	[X]	Limited connection / transfer
	X	Directional connection (source -> destination)

# Implementation: Phase 3

3. Identify & evaluate risks associated with local information flows
  - Greatest risk determined to be unauthorized disclosure of records
    - Identified independently by GLBA and FA
  - A. Evaluate identified risk(s)
    - Vectors include: Windows 98, local storage of assets, poor email authentication
  - B. Generate a risk-levels matrix
    - This step was added as a result of testing the Five Phases during the FA assessment
  - ✓ Acceptable risk levels determined





# Implementation: Phase 4

- 4. Develop mitigation strategy to address non-zero risk matrix elements
  - Existing policies mitigate network-borne attacks
  - Additional mitigations proposed to FA
    - Operating system upgrade
    - Alternatives to email for file transmission
    - Employ strong encryption (VPN, PGP, etc.)
  - ✓ Mitigation strategy developed



# Implementation: Phase 5A/B

## 5. Generate Final Risk Levels Matrix and Mitigations & Findings Reports

A. Re-evaluate remaining risk(s)

B. Generate final risk-levels matrix

- These two steps were added as a result of testing the Five Phases during the FA assessment





# Implementation: Phase 5C

## C. Generate mitigations & formal findings report

- Executive report
  - Recommendations presented in broad terms
  - Presented to FA liaison
- Technical report
  - Recommendations presented in more detailed terms
  - Presented to FA for their technical staff
  - Used by OIT to plan and deploy needed upgrades

✓ Final report complete



# Online Resources

- ◆ UMBC Information Services  
Risk Assessment Reference Site

<http://www.umbc.edu/oit/security/risk-assessment/>

- ◆ This Presentation

<http://userpages.umbc.edu/~robin/presentations.html>

